Quantum Entanglement and Quantum Computational Algorithms

Arvind *

February 1, 2008

Department of Physics,
Guru Nanak Dev University,
Amritsar, India 143 005

Abstract

The existence of entangled quantum states gives extra power to quantum computers over their classical counterparts. Quantum entanglement shows up qualitatively at the level of two qubits. We show that if no entanglement is envolved then whatever one can do with qubits can also be done with classical optical systems. We demonstrate that the one- and the two-bit Deutsch-Jozsa algorithm does not require entanglement and can be mapped onto a classical optical scheme. It is only for three and more input bits that the DJ algorithm requires the implementation of entangling transformations and in these cases it is impossible to implement this algorithm classically.

1 Introduction

The realisation that quantum-mechanical systems have a very large in-built information processing ability and can hence be used to implement computational algorithms has aroused much interest recently [1, 2, 3, 4, 5]. The basic unit of quantum information is the quantum bit (qubit), which can be visualised as a quantum two-level system. The implementation of quantum logic gates and circuits is based on the tenets of reversible logic and the fact that the two states of a qubit can be mapped onto logical 0 and 1 [6, 7, 8, 9]. Quantum mechanical realisation of logical operations can be used to achieve a computing power far beyond that of any classical computer [10, 11, 12, 13, 14]. A few quantum algorithms have been designed and experimentally implemented that perform certain computational tasks exponentially faster than their classical counterparts. Three such algorithms are, the Deutsch-Jozsa (DJ) algorithm [15], Shor's quantum factoring algorithm [16, 17], and Grover's rapid search algorithm [18].

The existence of entangled states within quantum mechanics is one of the most striking features of the theory [19]. These states have the potential to show nontrivial non-classical effects [20, 21, 22]. It is now well recognised that the EPR paradox is based on the existence of entangled states as only such states exhibit correlations that are capable of violating Bell's inequalities. It is rather interesting to note that entangled states play a crucial role

*arvind@physics.iisc.ernet.in

in quantum computation as well, and it is the entanglement between qubits that gives a quantum computer its inherent advantage. A few researchers have discussed quantum algorithms which do not rely on quantum entanglement and yet are still intrinsically quantum in nature; however such computations are not based on qubits [23].

We discuss in this paper how entanglement prevents the mapping or realisation of a quantum computation using classical waves alone. Consider the polarisation states of a classical light beam. These states are in one-to-one correspondence with the states of a qubit. All possible states can be realised by using one half-wave and two quarter-wave plates. One can thus pass from any desired polarisation state to all others in this way, i.e. all $U(2)$ transformations can be implemented using these gadgets [24]. Therefore a single qubit has a classical analogue. On the other hand, it is not possible to map all the states of a two-qubit system onto the polarisation states of two light beams. The entangled states of the two qubits have no classical counterpart. Therefore at the level of two qubits itself the possibility of mapping a quantum computer onto classical optical fields breaks down.

To mathematically define a quantum-entangled state, consider a system composed of two parts and described by a density matrix ρ. If the state of this system can be written in terms of the states of its constituent systems in one of the following ways then it is <u>not</u> entangled

$$\rho = \rho^1 \otimes \rho^2 \tag{1}$$

$$\rho = \sum_i \boldsymbol{p_i}\ \rho_i^1 \otimes \rho_i^2 \quad \text{with} \quad \boldsymbol{p_i}\ > 0. \tag{2}$$

In the case (1), the density matrix ρ comprises of the tensor product density matrices ρ_1 and ρ_2, describing the constituent subsystems. Each system has a complete quantum description by itself and ρ is said to be strongly separable. On the other hand, in the case (2) the density matrix ρ though not expressible as a tensor product of subsystem density matrices, is a positive sum of such tensor products. The positive coefficients $\boldsymbol{p_i}$'s can be interpreted as probabilities and therefore ρ can be thought of as a classical mixture of strongly separable pieces. Such a density matrix is termed weakly separable. However, if the state ρ is such that it cannot be expressed in either of the forms described in Eqns. (1) and (2), it is said to be entangled. For separable states the correlations present can be given a classical meaning by interpreting the positive coefficients $\boldsymbol{p_i}$'s as probabilities, an interpretation which is not possible for entangled states.

The central theme of this paper is to explore the scope of realising quantum computations on classical optical systems. In this context we demonstrate the fact that the DJ algorithm for up to two input bits is classical, since an explicit realisation of its implementation on a classical optical system based on polarisation is possible. Further we show that for more than two qubits the classical optical model fails since the algorithm essentially relies on quantum entanglement in this case. We stress that it is only at the level of three or more qubits that the DJ algorithm is a "truly quantum" algorithm.

2 The DJ algorithm

The DJ algorithm was one of the first algorithms that demonstrated the power of quantum computers over classical ones [15]. It determines whether a Boolean function f is constant or balanced. Classically, the algorithm requires many function calls to solve the problem without error. The quantum computer solves the problem using only a single function call.

Consider an n-bit binary string x; a function f can be defined on this n-bit domain space to a 1-bit range space, with the restriction that either the output is the same for all inputs (the function is constant) or the output is 0 for half the inputs and 1 for the other half (the function is balanced). All the 2^n possible input strings are valid inputs for the function ($f(x) = \{0, 1\}$). In quantum computation, these n-bit logical strings are in one-to-one correspondence with the eigenstates of n-qubits, and one can hence label the logical string x by the eigenstate $|x\rangle$. Classically, for an n-bit domain space, one needs to compute the function at least $2^{n/2} + 1$ times in order to determine whether it is constant or balanced. The DJ algorithm achieves this on a quantum computer using only a single function call [15, 25]. The original algorithm required the implementation of the function $f(x)$ encoded through a unitary transformation on an extra qubit, along with with the Hadamard transformation [15, 25].

The Hadamard transformation for n-qubits is given by

$$H^n|x\rangle = \sum_{y=0}^{2^n-1} (-1)^{\oplus \sum_j x_j y_j} |y\rangle \tag{3}$$

where x_j and y_j are the jth entries of the n-bit strings x and y and $\oplus$ symbolises addition modulo 2. The Hadamard transformation plays an important role in many quantum computational algorithms and when applied to the state $|0\rangle_{\text{n-bit}}$ generates a superposition of all possible eigenstates of the n qubit system. For a single qubit, the Hadamard transformation reduces to

$$\begin{array}{l} |0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array} ; H = H^{-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4}$$

The n-bit Hadamard transformation H^n is non-entangling in nature and is just a tensor product of n one-bit transformations.

A modified scheme can be designed to solve the n-bit Deutsch problem, using n qubits alone [26]. Here, for every function f a unitary transformation is constructed, such that its action on the eigenstates of n-qubits is

$$|x\rangle_{\text{n-bit}} \xrightarrow{U_f} (-1)^{f(x)} |x\rangle_{\text{n-bit}} \tag{5}$$

Consider n qubits, all in the state $|0\rangle$; a Hadamard transformation H^n converts this state to a linear superposition of all 2^n eigenstates with equal amplitudes and no phase differences. The unitary transformation U_f (defined in Eqn. 5) acting on this state, introduces an f-dependent phase factor in each eigenstate in the superposition. At this juncture, all information about f is encoded in the quantum state of the n qubits. A Hadamard transformation H^n is once again applied in order to extract the function's constant or balanced nature:

$$\begin{aligned} |0\rangle \xrightarrow{H^n} \sum_{x=0}^{2^n-1} |x\rangle \xrightarrow{U_f} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \xrightarrow{H^n} \\ \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)} (-1)^{\oplus \sum_j x_j y_j} |y\rangle \end{aligned} \tag{6}$$

The final expression for the output state in Eqn. 6 has an amplitude 1 for the state $|0\rangle_{\text{n-bit}}$ for a constant function and an amplitude 0 for a balanced function. The categorisation of the function as constant or balanced through a single function call using n qubits, is shown pictorially in Figure 1. The number of functions for the n-bit Deutsch problem is ${}^{N}C_{N/2}+2$

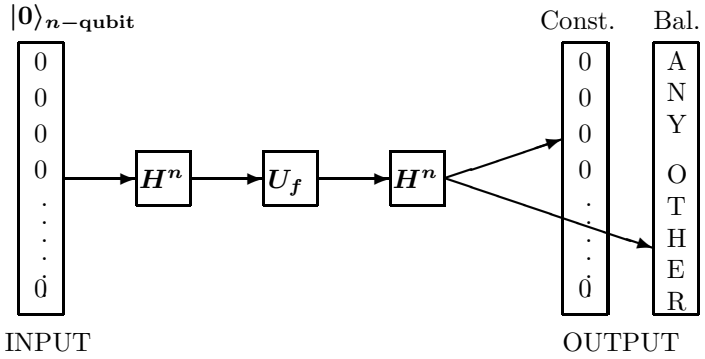

Figure 1: The block diagram for the modified DJ algorithm

(where $N = 2^n$). The experimental implementation of the modified DJ algorithm for n bits requires the realisation of the unitary transformation corresponding to each of these functions, and the n-bit Hadamard transformation, on a physical system. There have been many experimental implementations of the DJ algorithm and its modified version, using NMR [27, 28, 29, 30, 31, 32, 33].

3 Classical optical implementation of the DJ algorithm

We now proceed towards analysing this algorithm for 1 and 2 bits in detail, with a view to exploring the possibility of realising it on a classical optical system. Let us consider the following classical system: a monochromatic light beam propagating in a given direction with a pure polarisation. The polarisation states of such a beam are in one-to-one correspondence with the states of a two-level system and this beam can therefore be visualised as a qubit. It is also well known that all unitary transformations on the polarisation states can be performed. Consider a birefringent plate with its thickness adjusted to introduce a phase difference of η between the x and y components of the electric field and whose slow axis makes an angle ϕ with the x axis. The unitary operator corresponding to this plate is given by

$$U(\eta,\phi) = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} e^{i\eta/2} & 0 \\ 0 & e^{-i\eta/2} \end{pmatrix} \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} \tag{7}$$

For the choice $\eta = \pi$ it becomes a half-wave plate and we denote it by H_ϕ, while for $\eta = \pi/2$ it becomes a quarter-wave plate and we denote it by Q_ϕ. It has been shown that all $SU(2)$ transformations can be realised on the polarisation states by taking two quarter-wave plates and one half-wave plate with suitable choices of angles of their slow axes with the x axis.

We will henceforth refer to this device capable of implementing $SU(2)$ transformations as Q-H-Q and a detailed discussion is found in [24].

Further, let us map the x polarisation state to logical 1 and the y polarisation state to logical 0. With this mapping we can proceed to work with this system as a qubit. Since this system comprises essentially of classical elements, we call it a "classical qubit".

One-bit case: For the purpose of implementing the one-bit DJ algorithm on a "classical qubit", we need to realise the Hadamard transformation H which corresponds to an anti-clockwise rotation of polarisation by 45^0 in the $x-y$ plane and the four U_f transformations corresponding to the four possible functions. These are certain $SU(2)$ transformations and therefore are implementable using the Q-H-Q device discussed above. The sequence of optical operations is detailed in Figure 2. As an example, consider the third unitary transformation

$$U_3^{1-\text{bit}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{8}$$

which when realised on a "classical qubit" would leave the y polarisation unaffected while the x polarisation picks up a phase factor of $e^{i\pi}$. This transformation is achievable by a single half-wave plate.

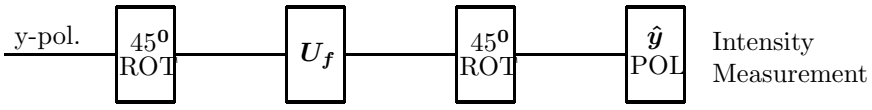

Figure 2: Optical realisation of 1-bit DJ algorithm. If the resultant polarisation after the second 45^0 rotation is along $\hat{y}$ then the function is constant and if it is along x the function is balanced. Since these two polarisation states are orthogonal it is possible to distinguish them with certainty by placing a y polarizer after the second 45^0 rotation, followed by an intensity measurement.

The outcome of this exercise is to show that there is nothing quantum about this procedure, and that the concept of a qubit can be mapped onto the polarisation states of a light beam.

Two-bit case: For implementing the two-bit DJ algorithm, we consider two beams of monochromatic light representing two "classical qubits". The Hadamard transformation H^2 is again a rotation of the polarisation of both the beams in the anti-clockwise direction by an angle of 45^0. All the eight $U_f^{2-\text{bit}}$ transformations corresponding to the eight functions turn out to be factorisable as a direct product of two $SU(2)$ transformations, one acting on each qubit.

$$U_f^{2-\text{bit}} = U_f^1 \otimes U_f^2 \quad \text{with} \quad U_f^1, U_f^2 \in SU(2) \tag{9}$$

More specifically we give in Eqn. 10 the decomposition of four of the eight functions. The other four transformations differ from these four by an overall phase factor of π and therefore can be similarly factorised.

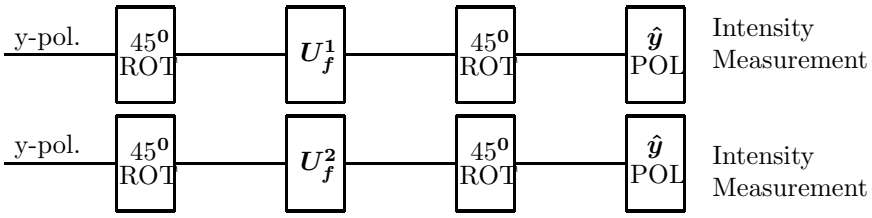

Figure 3: Optical realisation of the DJ algorithm for two qubits. Similar to the one-bit case, the polarisers along $\hat{y}$ are placed after the final Hadamard transformation to project out the $|00\rangle$ state. The presence of light signal in both the beams indicates a constant function while the absence of signal in either of the beams indicates a balanced function.

$$
\begin{aligned}
U_1^{2-\text{bit}} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} &&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} && \text{No Operation} \\
U_2^{2-\text{bit}} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} &&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} && \text{HWP on 1st beam} \\
U_3^{2-\text{bit}} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} &&= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} && \text{HWP on 2nd beam} \\
U_4^{2-\text{bit}} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} &&= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} && \text{HWP on both beams}
\end{aligned}
\tag{10}
$$

To implement these transformations on two "classical qubits" requires insertion of a half wave plate in one or both beams and can be achieved in a straightforward way. Hence the implementation of $U_f^{2-\text{bit}}$ can be achieved by applying the required $SU(2)$ transformation on each qubit separately. The schematic diagram of this implementation is shown in Figure 3.

4 Entanglement at the three-qubit level

We now turn to the case of three input qubits. In this case too the Hadamard transformation H^3 corresponds to a 45^0 rotation of the polarisations of each of the three qubits and can be implemented easily. The functions $U_f^{3-\mathrm{bit}}$ are 72 in number and any physical implementation would require a prescription to implement all of them on a system of three qubits. Consider for example, a particular balanced function given by the 8×8 diagonal matrix

$$U_f = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{11}$$

This simple looking $SU(8)$ diagonal matrix cannot be written as a direct product of $SU(2)$ matrices acting on individual qubits!. This transformation is entangling in nature and possesses the capacity to generate entangled states from non-entangled ones. To see this clearly, let us consider the action of this matrix on a simple un-entangled initial state

$$U_f \frac{1}{2\sqrt{2}} \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \\ -1 \\ -1 \\ -1 \\ 1 \end{pmatrix} \tag{12}$$

The entanglement of this final pure three-qubit state can be demonstrated by computing the reduced density matrix for the last two qubits, by taking a partial trace over the first qubit

$$\begin{aligned} \rho^{2-3} &= \frac{1}{4} \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \\ \text{where} (\rho^{2-3})^2 &\neq \rho^{2-3} \end{aligned} \tag{13}$$

The result $(\rho^{2-3})^2 \neq \rho^{2-3}$ implies that the reduced density matrix is mixed, proving the entangled nature of the overall state of the 3-qubit system. The question now arises as to how do we realise such an entangling transformation for our "classical qubit" system? It turns out that there is no way we can realise such transformations on "classical qubits". It is to be noted that there are $SU(2) \otimes SU(2) \otimes SU(2)$ worth of states for the system of three "classical qubits" under consideration and this does not contain the entangled states. As shown above, entangling transformations on the other hand, generate entangled states from non-entangled ones and therefore there is no possibility of being able to construct and implement them on

this system of "classical qubits". Hence in order to implement the three bit DJ algorithm we need a *real quantum-mechanical three-qubit* system. Such implementations have been discussed in the context of liquid state NMR quantum computing [27, 28, 29, 30, 31, 32, 33].

5 Concluding Remarks

A complete mapping of a qubit exists in the classical world of polarisation optics. We can consider $SU(2)$ worth of pure polarisation states of a monochromatic beam of light as a qubit. All unitary operations required to implement logical operations being $SU(2)$ transformations, can be implemented through Q-H-Q. We have shown that the one-bit DJ algorithm can be readily implemented on this system. More generally, we can say that every operation which can be conceived of for a single qubit, can be executed on this classical system.

We have shown that for more than one qubit the "classical qubit" system can work for those computations which do not involve entanglement and for such cases there might be an advantage over the ordinary binary computers. In particular for the two-bit DJ algorithm, since it does not involve quantum entanglement in its implementation for two bits, we are able to realise it on our "classical qubits". This algorithm for the two-bit case solves the problem with only one function call as opposed to the ordinary classical algorithm requiring three function calls. Hence even when this algorithm allows a realisation based on the "classical qubits" it outperforms the algorithm based on ordinary binary logic. Therefore, using a pair of "classical qubits" has some advantage!

Finally we illustrate that an algorithm becomes a true quantum algorithm only when it involves quantum entanglement at some stage of its implementation, otherwise it is implementable on a set of "classical qubits". The DJ algorithm for three qubits has been shown to involve entangled states for its implementation. Therefore, it becomes impossible to realise its implementation using "classical qubits".

Acknowledgements: I thank my collaborators Kavita Dorai, Anil Kumar, N. Mukunda and R. Simon for useful discussions.

References

[1] D. P. DiVincenzo, Science, **270**, 255 (1995).

[2] C. H. Bennett, Phy. Today., **273**, 44 (1995).

[3] I. L. Chuang, R. Laflamme, P. W. Shor, and W. H. Zurek, Science, **270**, 1633 (1995).

[4] J. Preskill, LANL preprint, quant-ph/9705032.

[5] C. H. Bennett and D. P. DiVincenzo, Nature, **404**, 247 (2000).

[6] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[7] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

[8] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Phys. Rev. Lett., **75**, 4714 (1995).

[9] D. P. DiVincenzo, Proc. Roy. Soc. London A, **454**, 261 (1998).

[10] C. H. Bennett, IBM Jl. Res. Develop., **17**, 525 (1973).

[11] R. P. Feynmann, Int.J.Theor.Phys., **21**, 467 (1982).

[12] P. Benioff, Phys. Rev. Lett., **48**, 1581 (1982).

[13] D. Deutsch, Proc.Roy.Soc.London A, **400**, 97 (1985).

[14] D. Deutsch, Proc. Roy. Soc. London A, **425**, 73 (1989).

[15] D. Deutsch, and R. Jozsa, Proc. Roy. Soc. London A, **439**, 553 (1992).

[16] P. W. Shor, SIAM J. Comput., **26**, 1484 (1997).

[17] A. Ekert and R.Jozsa, Rev. Mod. Phy., **68**, 733 (1996).

[18] L. K. Grover, Phys.Rev.Lett. **79**, 325 (1997).

[19] E. Schroedinger, Proc.Camb.Phil.Soc., **31**, 555 (1935).

[20] A. Ekert and P. L. Knight, Am. J. Phys., **63**, 415 (1994).

[21] A. Peres, Phys.Rev.Lett., **77**, 1413 (1996).

[22] P. Horodecki, Phys.Lett.A, **232**, 333 (1997).

[23] S. Lloyd, Phys.Rev.A, **61**, 010301/1-4 (2000).

[24] R. Simon and N. Mukunda, Phys.Lett.A, **143**, 165 (1990).

[25] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc.Roy.Soc.London A, **454**, 339 (1998).

[26] D. Collins, K. W. Kim, and W. C. Holton, Phys.Rev.A, **58**, R1633 (1998).

[27] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung, and S. Lloyd, Nature, **393**, 143 (1998).

[28] J. A. Jones and M. Mosca, J. Chem. Phys., **109**, 1648 (1998).

[29] N. Linden, H. Barjat, and R. Freeman, Chem.Phys.Lett., **296**, 61 (1998).

[30] Kavita Dorai, Arvind, and Anil Kumar, Phys.Rev.A, **61**, 042306/1-7 (2000).

[31] Arvind, Kavita Dorai, and Anil Kumar, LANL preprint, quant-ph/9909067.

[32] J. Kim, J. Lee, S. Lee, and C. Cheong, LANL preprint, quant-ph/9910015.

[33] Dong Pyo Chi, Jinsoo Kim, Sooyoon Lee, LANL preprint, quant-ph/0005059.